II. AMENDMENTS TO THE CLAIMS

The following listing of claims replaces all prior versions, and listings, of claims in the application:

1. (Currently Amended) A method for protecting a distributed application user, comprising:

providing a distributed application on a server;

~~determining~~ generating a security value for an authenticated user of the distributed application, wherein every user is authenticated prior to generating the security value and the security value is a pseudo-random number;

associating the security value with a set of commands of the distributed application, wherein each command comprises a command that can be used in a malicious attack against the authenticated user;

receiving one of the set of commands on the server from the authenticated user;

checking the one command for the security value to determine if the one command originated from the authenticated user;

preventing execution of the one command if the security value is not found with the one command; and

returning an error message to the authenticated user if the security value is not found with the one command, wherein the error message prompts the authenticated user for confirmation before the one command can be executed.

2. (Previously Presented) The method of claim 1, wherein the one command comprises a command to delete files of the authenticated user.

3. (Canceled).

4. (Currently Amended) The method of claim 1, wherein the security value, as [[is]] a pseudo-random number, is generated by a random number generator.

5. (Original) The method of claim 1, further comprising storing the security value on the server.

6. (Original) The method of claim 1, further comprising:

associating the security value with session information corresponding to the authenticated user; and

communicating the session information and the security value to the authenticated user.

7. (Original) The method of claim 1, wherein the authenticated user operates a client that communicates with the server.

8. (Original) The method of claim 7, wherein the associating step comprises appending the security value to a set of uniform resource locators (URLs) that correspond to a set of commands of the distributed application, and wherein the receiving step comprises receiving one of the set of URLs on the server from the authenticated user.

9. (Original) The method of claim 8, wherein the one URL is pre-constructed on the server.

10. (Original) The method of claim 8, wherein the one URL is constructed on the client, and wherein the method further comprises:

extracting the security value on the client; and

appending the security value to the one URL on the client.

11. (Currently Amended) A method for protecting a distributed application user, comprising:

providing a distributed application on a server;

authenticating a user of the distributed application, wherein every user is authenticated;

~~determining~~ generating, on the server, a security value for the authenticated user, wherein the security value is a pseudo-random number;

associating the security value with a set of uniform resource locators (URLs) corresponding to a set of commands of the distributed application, wherein each command comprises a command that can be used in a malicious attack against the authenticated user;

communicating the security value to a client operated by the authenticated user;

receiving one of the set of URLs on the server from the client;

checking the one URL for the security value to determine if the one URL originated from the authenticated user;

preventing execution of the command corresponding to the one URL if the security value is not found with one URL; and returning an error message to the authenticated user if the security value is not found with the one URL, wherein the error message prompts the authenticated user for confirmation before the one URL can be executed.

12. (Previously Presented) The method of claim 11, further comprising wherein the one URL is associated with a command to delete files of the authenticated user.

13. (Original) The method of claim 11, further comprising:

determining session information for the authenticated user; and

associating the security value with the session information, wherein the communicating step comprises sending the session information and the security value to a client operated by the user.

14. (Original) The method of claim 11, wherein the associating step comprises appending the security value to a set of URLs corresponding to a set of commands of the distributed application.

15. (Original) The method of claim 11, wherein the one URL is pre-constructed on the server, and wherein client receives the one URL and the associated security value from the server.

16. (Original) The method of claim 11, wherein the one URL is constructed on the client, and wherein the associating step comprises;

extracting the security value on the client; and

appending the security value to the one URL.

17. (Original) The method of claim 11, further comprising storing the security value on the server, prior to communicating the security value to the client.

18. (Currently Amended) A system for protecting a distributed application user, comprising:

a computer device including:

a security value system for ~~determining~~ generating a security value for an authenticated user of a distributed application provided on a server, wherein every user is authenticated prior to generating the security value and the security value is a pseudo-random number;

an association system for associating the security value with a set of commands of the distributed application, wherein each command comprises a command that can be used in a malicious attack against the authenticated user; and

a command checking system for checking one of the set of commands received on the server from the authenticated user for the security value to determine if the one command originated from the authenticated user, for preventing execution of the one command if the security value is not found with the one command, and for returning an error message to the authenticated user if the security value is not found with the one command, wherein the error message prompts the authenticated user for confirmation before the one command can be executed.

19. (Previously Presented) The system of claim 18, wherein the one command comprises a command to delete files of the authenticated user.

20. (Original) The system of claim 18, further comprising an authentication system for authenticating a user of the distributed application.

21. (Currently Amended) The system of claim 18, wherein the security value, as [[is]] a pseudo-random number, is generated by a random number generator.

22. (Original) The system of claim 18, wherein the security value is stored on the server.

23. (Original) The system of claim 18, wherein the security value is associated with session information corresponding to the authenticated user, and wherein the session information and the associated security value are communicated to the authenticated user.

24. (Original) The system of claim 18, wherein the command checking system comprises a filter servlet.

25. (Original) The system of claim 18, wherein the authenticated user operates a client that communicates with the server.

26. (Original) The system of claim 25, wherein the association system appends the security value to a set of uniform resource locators (URLs) that correspond to a set of commands of the distributed application, and wherein the command checking system checks one of the set of URLs received on the server from the authenticated user for the security value.

27. (Original) The system of claim 26, wherein the one URL is pre-constructed on the server.

28. (Original) The system of claim 26, wherein the one URL is constructed on the client, and wherein the client comprises a command system for extracting the security value on the client, and for appending the security value to the one URL.

29. (Currently Amended) A computer program product stored on a computer readable medium for protecting a distributed application user, which when executed, comprises:

program code for ~~determining~~ generating a security value for an authenticated user of a distributed application provided on a server, wherein every user is authenticated prior to generating the security value and the security value is a pseudo-random number;

program code for associating the security value with a set of commands of the distributed application, wherein each command comprises a command that can be used in a malicious attack against the authenticated user; and program code for checking one of the set of commands received on the server from the authenticated user for the security value to determine if the one command originated from the authenticated user, for preventing execution of the one command if the security value is not found with the one command, and for returning an error message to the authenticated user if the security value is not found with the one command, wherein the error message prompts the authenticated user for confirmation before the one command can be executed.

30. (Previously Presented) The computer program product of claim 29, wherein the one command comprises a command to delete files of the authenticated user.

31. (Previously Presented) The computer program product of claim 29, further comprising program code for authenticating a user of the distributed application.

32. (Currently Amended) The computer program product of claim 29, wherein the security value, as [[is]] a pseudo-random number, is generated by a random number generator.

33. (Previously Presented) The computer program product of claim 29, wherein the security value is stored on the server.

34. (Previously Presented) The computer program product of claim 29, wherein the security value is associated with session information corresponding to the authenticated user, and wherein

the session information and the associated security value are communicated to the authenticated user.

35. (Previously Presented) The computer program product of claim 29, wherein the program code for checking comprises a filter servlet.

36. (Previously Presented) The computer program product of claim 29, wherein the authenticated user operates a client that communicates with the server.

37. (Previously Presented) The computer program product of claim 36, wherein the program code for associating appends the security value to a set of uniform resource locators (URLs) that correspond to a set of commands of the distributed application, and wherein the program code for checking checks one of the set of URLs received on the server from the authenticated user for the security value.

38. (Previously Presented) The computer program product of claim 37, wherein the one URL is pre-constructed on the server.

39. (Previously Presented) The computer program product of claim 37, wherein the one URL is constructed on the client, and wherein the client comprises a program code for extracting the security value on the client, and for appending the security value to the one URL.